大和高田市情報セキュリティシステム一式調達仕様書

1．件名　　　　　平成25年度情報セキュリティシステム一式リース契約に係る納入業者決定

2．納入場所　　　大和高田市役所内　大和高田市大字大中100番地1

3．納入期限　　　平成25年9月21日

4．リース期間　　平成25年10月1日～平成30年9月30日
　保守期間　　　平成25年10月1日～平成30年9月30日

5．導入の背景

昨今の高度情報化社会において、情報の漏洩・不正流出は最も重要視すべき課題の一つとなっている。本市においても、取り扱う情報には住民の個人情報をはじめ、行政上重要な情報など、外部に漏洩した場合、極めて重大な問題となる情報が多く含まれている。

したがって、情報資産を様々な脅威から守り、市民の個人情報を保護することは、市民からの信頼を確保するとともに、安定的な行政運営に寄与する。このような背景により、本事業は、情報漏洩のリスクが高いと考えられる以下の内容を主として対策を実施するものである。

（1）外部記憶媒体使用制限／IT資産管理
（2）添付メール対策／メール検閲
（3）Webフィルタリング

6．基本仕様

（1）導入後の迅速な保守のため、現地での訪問修理が可能であり、導入後5年間は修理に必要な部品を無償で提供できるパーツ保証を実施できること。
（2）各機器については、「国等による環境物品等の調達の推進等に関する法律」に準拠したものであること。
（3）各機器については、必要以外のサービスの停止、最新のセキュリティパッチの適用などのセキュリティ対策を施した機器であること。
（4）機器の全てについて、必然的に必要となる物品については、仕様書記載の有無にかかわらず、全て納入すること。

7. 機器の仕様　　サーバ情報

（1） クライアント情報

［情報系］

・クライアント数：約100台

・クライアントOS：WindowsXP（SP2 以上）及びWindows7（SPなし、SP1）

・想定同時アクセス数：約100台（ストレスなくWeb閲覧、メール利用が可能なこと）

・Windows Server 2012 DeviceCAL：情報系の100台については必要クライアント数を保有していない為、調達対象とする。

［基幹系］

・クライアント数：約540台

・クライアントOS：WindowsXP（SP2 以上）及びWindows7（SPなし、SP1）

・想定同時利用数：約540台（導入する機能が既存のシステムの動作に影響を与えないこと）

・Windows Server 2008 DeviceCAL：広報情報課が必要クライアント数を保有（調達不要）

（2） 今回調達する機器は、広報情報課既設の19インチラックに格納できること（参考搭載予定ラック型番：N8140－94）

（3） ハードウェア仕様

①IT資産管理システム用サーバ【基幹系サーバ】

本市にて別途調達するサーバを利用すること。

サーバはOSセットアップが完了した状態での引き渡しとなるため、OSセットアップ以外のサーバ稼働に必要な導入作業を全て行うこと。なお、上記記載の物品以外にシステム導入に必要な物品があれば今回の調達に含むこと。

IT 資産管理システム用に専用の外部ストレージ（②）を用意し、サーバデータ等の外部バックアップを実現すること。専用のリカバリメディアを使って、初期納品時の状態へリストアできる体制を作ること。

参考:基幹系サーバ参考スペック(調達対象外)

形状	2U ラックマウント
OS	Windows Server 2008 R2 Standard
CPU	Xeon E5-2609(4Core/2.4GHz)相当
HDD	300GB(SAS 10000rpm)×3台　RAID 5(WriteBack 設定)相当
RAID カード	RAID5 対応、メモリ 512MB 以上、バックアップ用バッテリ搭載
メモリ	8GB　サーバ用途の DIMM(Registered DIMM 等)
内蔵光学ドライブ	DVD-ROM/CD-ROM の読込が可能
LAN	1000BASE-T/100BASE-TX/10BASE-T×2以上
電源	冗長化されている
筐体ファン	冗長化されている
USB	USB2.0 準拠、前面/背面合計で6ポート備えている
UPS	ラックマウント2U サイズ、100V/1500VA/1200W 相当 管理ソフトウェアを搭載し、電源障害発生時において安全に自動シャットダウンできる。また業務時間外にサーバの自動シャットダウン及び自動起動が可能。
ﾘﾑｰﾊﾞﾌﾞﾙﾄﾞﾗｲﾌﾞ	HDD のシステム領域・データ領域を週 5 日、システムを停止することなく業務時間外にリムーバブルメディアにバックアップできる。
ウイルス対策	本市にて別途準備するウイルス対策ソフトウェアのクライアントモジュールを導入する。 (ウイルスバスターコーポレートエディション又は ServerProtect)
コンソール	既設のサーバスイッチユニットへ接続する。

②IT資産管理システム用外部ストレージ【基幹系サーバ】

HDD	IT 資産管理システム用サーバのログやデータのバックアップを格納できるようすること。過去 5 年間のログやデータを保管して運用管理できるよう設定すること。
UPS	電源障害発生時において安全に自動シャットダウンできるようすること。
バックアップ	本ストレージに格納する全てのバックアップデータが退避可能な容量を有するUSBハードディスクを用意し、本ストレージのバックアップを退避すること。
その他	Active Directory 連携可能な製品とし、IT 資産管理システムの管理プログラムを利用して、本ストレージ内の過去年度データに対するアクセスコントロールを実現できること。 電源障害発生時において安全に自動シャットダウンができるようにすること。

③セキュリティUSBメモリー

個数	100個
容量	2GB以上
仕様	今回調達する資産管理システムに対応している製品であること。 USBメモリは暗号化のためのソフトウェアが附属しており、接続時にパスワードを入力しなければアクセスできないようになっていること。 USBメモリ個体ごとにシリアルナンバーが格納されていること。 指定された端末でのみ使用できる機能を備えていること。
その他	USBメモリにはストラップホールがついていること。 また、ストラップを個数分用意すること。

④Webフィルタリング用サーバ【情報系サーバ】

形状	2U 以内ラックマウント
CPU	Xeon E3-1220v2 (4C/3.10GHz/8M)相当以上
HDD	300GB(SAS 10000rpm)×2 台 RAID1 300GB(SAS 10000rpm)×1 台(HS) (ホットスペア×1 を用意し RAID 障害時に、自動的に本番ディスクへ昇格する) 上記スペック相当以上。同等以上のパフォーマンスと信頼性を確保できるのであれば、RAID5+ホットスペア構成でも可とする。 ※ログ保管の項目を参照し、必要があれば内蔵ディスク容量追加すること。
メモリ	8GB サーバ用途の DIMM(RDIMM 等)
光学ドライブ	DVD-ROM/CD-ROM の読込が可能なこと。
LAN	1000BASE-T/100BASE-TX/10BASE-T 対応×2 ポート以上
USB	USB2.0 準拠、前面/背面合計で6ポート備えていること。
OS	Windows Server 2008 R2 Standard 又は、 Windows Server 2012
CAL	Windows Server 2012 デバイス CAL 100 ライセンス
ウイルス対策	本市にて別途準備するウイルス対策ソフトウェアのクライアントモジュールを導入すること。 (ウイルスバスターコーポレートエディション、又は Server Protect)
UPS	2U サイズ以内 100V/1500VA/1200W 相当以上 管理ソフトウェアを搭載し、電源障害発生時において安全に自動シャットダウンできるようすること。
容量 (ログ保管)	クライアント 100 台環境において、5 年間のログやデータをサーバ内部に保存できる十分な容量を確保すること。
バックアップ	バックアップ用の外部ストレージを用意し、サーバ内のログやデータの外部バックアップを実現すること。IT 資産管理システムとは所属するネットワークが異なるので共用は不可とする。
リカバリイメージ作成	リカバリメディアを使って、初期納品時の状態へリストアできる体制を作ること。
コンソール	既設のサーバスイッチユニットへ接続するケーブル(3m 以上)を調達すること。

⑤メールフィルタリングおよびメールアーカイブ用サーバ【情報系サーバ】

形状	2U 以内ラックマウント
CPU	Xeon E3-1220v2 (4C/3.10GHz/8M) 相当以上
HDD	450GB(SAS 10000rpm)×3 台 RAID5 450GB(SAS 10000rpm)×1 台(HS) (※ホットスペア×1 を用意し RAID 障害時に、自動的に本番ディスクへ昇格する) 上記スペック相当以上 ※ログ保管の項目を参照し、必要があれば内蔵ディスク容量追加すること。
メモリ	8GB サーバ用途の DIMM(RDIMM 等)
光学ドライブ	DVD-ROM/CD-ROM の読込が可能なこと。
LAN	1000BASE-T/100BASE-TX/10BASE-T 対応×2 ポート以上
USB	USB2.0 準拠、前面/背面合計で6ポート備えていること。
OS	Windows Server 2008 R2 Standard 又は、 Windows Server 2012
ウイルス対策	本市にて別途準備するウイルス対策ソフトウェアのクライアントモジュールを導入すること(ウイルスバスターコーポレートエディション、又は Server Protect)
UPS	2U サイズ以内 100V/1500VA/1200W 相当以上 管理ソフトウェアを搭載し、電源障害発生時において安全に自動シャットダウンできるようすること。
ログ保管	クライアント 100 台環境において、5 年間のログやデータをサーバ内部に保存できる容量を確保すること。
バックアップ	バックアップ用の外部ストレージを用意し、サーバ内のログやデータの外部バックアップを実現すること。IT 資産管理システムとは所属するネットワークが異なるので共用は不可とする。
リカバリイメージ作成	リカバリメディアを使って、初期納品時の状態へリストアできる体制を作ること。
コンソール	既設のサーバスイッチユニットへ接続するケーブル(3m 以上)を調達すること。

（4） 設置場所

ア. 今回調達する機器は、本庁サーバ室に設置

イ. 本庁 LAN 構成

サーバ室 ～ 各階メインハブ間は1，000Mbps

各階メインハブ ～ 原課設置端末間は100Mbps

ウ. 出先ネットワーク構成

サーバ室 ～ 出先機関との回線速度は100Mbps

出先機関内のLANは100Mbps

（5） 今回調達する機器について、異常発生時はサーバ管理者への通知（メール、連絡等）が可能であること。また、機器前面のパネル等により障害の原因が特定できること。

（例）ハードディスク異常、バッテリ交換が必要等

（6） 電源障害や停電発生時に、今回調達するUPSにて5分以上サーバを稼動させることが可能であり、システムを安全に停止できること。また、復旧した際にはシステムを自動で起動できること。

（7） 今回調達する機器について、保守期間内に搭載バッテリ（RAID ボード、UPS 等）等の交換が必要となった場合は、その交換機器費用及び交換作業費用を保守業者にて負担すること。

（8）サーバラックは、既設の19インチラック（24Uタイプ）を利用し、2U＋5U以内で収めること。なお、画面操作を必要とする場合は、既設のサーバスイッチユニットへ接続するケーブル（3m以上）を調達すること。

8. ソフトウェアの仕様

（1）外部記憶媒体使用制限／IT資産管理

■基本要件

ア. クライアント管理ソフトウェアの仕様及び機能については、安定稼働の観点から、本調達の仕様書公告時点において開発が完了しており、導入実績があるもの以外は一切認めないものとする。

イ. クライアント管理ソフトウェアの仕様及び機能については、安定稼働・サポートの観点から、

フリーソフトウェア及びシェアウェアソフトでの実現は不可とする。

ウ. 本ソフトウェアは使用頻度が高いことが見込まれ、保守契約期間中において電話/E-Mailによるメーカー直接の問合せ対応ができ、マイナー/メジャーバージョンアップ/後継品を問わず、常に最新版のプログラム提供を行うこと。

エ. クライアントの対応 OS については、Microsoft WindowsXP、Windows Vista、Windows 7、Windows8 に対応していると共に、保守契約期間中については、最新 OS 対応を無償で行うこと。

■資産管理

ア. 他のオプション等の製品と連携することで、SNMP によるネットワーク機器情報の取得及び各クライアントからのインベントリ情報(コンピュータ名、ネットワーク情報等)の自動収集・一覧表示ができること。

イ. IT 資産管理台帳として、インストールソフトウェア台帳・ソフトウェアライセンス台帳・ハードウェア台帳の3つの台帳で管理が行えること。

ウ. クライアント上のソフトウェアに関するインストール状況を収集する機能を有すること。収集できる内容としては、以下の通りとする。また、クライアントごとにアプリケーション状況を把握できること。

収集対象:アプリケーションインストール状況・OS ライセンス情報・Office インストール状況(OpenOffice、MicrosoftOffice 含む)・ウィルス対策ソフトウェアインストール状況・Windows 更新プログラム適用状況、Windows ストアアプリインストール状況 Office アプリケーション(MicrosoftOffice)の GUID、バージョン、インストール日付

エ. ソフトウェア自動配布が可能であり、ソフトウェア自動配布以外にも、ソフトウェアの自動実行、レジストリの自動編集などができること。また、ユーザー権限の端末に対しても、管理者権限でログインしなおすことなく自動的にソフトウェアがインストールできること。

オ. ファイルの配布、ソフトウェアの自動インストール及び任意プログラムの実行をする際、ユーザ側にソフトウェアがインストール中である等の表示(及び非表示)が行える機能を有すること。

カ. 特定及び複数のクライアントまたは、グループに対して、アンケートが行えること。

■制限・制御・アラート管理

ア. 利用者による禁止アプリの名前変更の禁止又はウィンドウタイトルによるアプリ起動禁止が可能なこと。

イ. 事前定義されたルールに反した際に、通知する機能、もしくは操作を禁止する機能について、設定したグループごとに設定できること。

ウ. 収集したログについて特定の行為及び内容から、事前定義されたルールに従い、自動的に管理者へアラートをメール等で通知する機能を有すること。設定できる項目について

は、次の通りとする。

設定項目：ウィンドウタイトル・アプリケーション実行・アプリケーションの名前変更・レジストリ変更・インストール・システム構成変更・CSV ファイル出力・規定時間外端末機操作・記憶媒体使用・CD-R/DVD-R 書き込み・記憶媒体書き込み、・特定フォルダアクセス・ドライブ追加・共有フォルダ書き込み・ローカル共有フォルダ作成・ローカル共有フォルダアクセス

■USB デバイス管理（「基幹系」及び「情報系」）

ア. USB 外部ストレージをクライアントもしくは管理者のクライアントに挿入した際、利用したUSBメモリのメーカー名、シリアルナンバー、ベンダーIDを自動で収集し、管理台帳を作成できること。また、利用者や所属部署、管理番号などを任意で入力できること。収集した情報にもとに指定した USB メモリを使用許可／不許可／読み取り専用を設定できること。使用許可／不許可／読み取り専用の設定は、ネットワーク全体および指定した部署のみ利用可など柔軟な設定が行えること。

イ. USB デバイスがコンピュータに装着された日時を取得できること。

ウ. USB デバイスがコンピュータに装着されたログを絞り込み、特定の期日以前のログを持つデバイスを使用禁止にできること。

エ. ファイル操作とUSBを利用したログを絞り込むなどして、USBメモリの最終使用時に、どのようなファイルが保存されていたかを調査することが可能なこと。

オ. 1つの USB デバイスを複数部署で使用する場合、部署ごとに使用許可/使用不可能/書き込み禁止を設定できること。

■ログ取得

ア. クライアントに対して行われた操作、ログオン、ログオフの日時、実行されたソフトウェアについての起動・終了時間、ファイル操作、共有フォルダへのアクセス・ファイル操作、クリップボードにコピーされた内容、USB メモリなどの記憶媒体を利用した内容および記憶媒体のシリアル情報等を記録する機能を有すること。

イ. 収集されたファイル操作ログから、一つのファイルに対して、どのような操作（コピー、ファイル名変更、新規作成、削除など）が行われたかを抽出して表示する機能を有すること。また、Microsoft Office 製品については名前を付けて保存（別ファイル名保存）ログを取得・表示できること。

ウ. 特定の操作ログより特定の時間を指定しての操作ログを検索する機能を有すること。

エ. 外部ストレージ上にバックアップとして保存されたログについては、閲覧する際に簡単な操作でログを復元して、管理コンソール等、専用画面から検索し、閲覧することが可能であること。

オ. 後述するリモート操作を行った履歴及び管理者側が行った操作としてログが残せること。

カ. クライアントコンピュータが Windows の「最近使ったファイル」のアプリケーションのファイル

を開く操作をログとして記録する機能を有すること。また、事前定義されたキーワードが含まれているファイルが開かれた場合は、管理者へ自動的にメール等でアラート通知する機能を有すること。

キ. ログについては改ざん防止のため、一時的にクライアントに保持している間も暗号化して保存されること。

■リモート操作

ア. vPro 対応・設定されている、また、WOL を利用できる場合に、特定のクライアントに対して、電源の管理が行え、ネットワーク経由でキー及びマウス操作をリモートで行える機能を有すること。

イ. 管理コンソールからクライアントに対してファイルのコピーができること。

ウ. 通信帯域を制限できること。また、リモート操作で画面を受信する際、画質等を落として通信データ量を抑制できること。遠隔操作の操作状況に応じて、遠隔操作中の通信量をコントロールする機能を有すること。

エ. Windows 端末の 2 画面以上のディスプレイを同時に使用しているクライアントに対してリモート操作を行う場合、操作するディスプレイを切り替えて対応できる機能を有すること。

■管理コンソール

ア. 本要求仕様項目については、OS 動作中に常に動作・常駐するソフトウェアの動作上、複数メーカーの製品を組み合わせることは、コンピュータ自体が不安定になる可能性が捨てきれないため、メーカーが、一つの製品として提供しており、運用面も考慮し、1 つの管理コンソール上から上記機能要件が全て操作できること。

イ. よく使用する機能を登録できクイックアクセスができるような機能があること。

ウ. ボタンの機能の簡易説明が表示される機能を有すること。

エ. 端末の操作画面を管理端末で表示する際に、アラート未発生端末の操作画面は非表示とする、プライバシー保護に配慮した機能を有すること。不正操作及び誤操作発生時に、早期の問題把握ができる機能を有すること。

オ. セキュリティの観点から、管理コンソールは「Web ベースまたはプログラムで実行できること。

(2)添付メール／メール検閲対策

ア. メールセキュリティはメールの全文保存と、誤送信対策としてルール付けができること。誤送信対策は添付ファイルを自動でパスワードロック(ZIP 形式)することが可能であること。また、セキュリティポリシーによってはより強固な暗号化強度を確保できるようにするため基本の機能で AES(Advanced Encryption Standard) 256bit 形式で添付ファイルの暗号化が可能であること。

イ. 送信メールを即時送信せず、一定時間滞留させることが可能であり、さらに滞留させる場

合でも、誤送信であることが送信者本人以外でも確認できるように宛先に内部ドメインが含まれている場合、その宛先には即時送信が可能なこと。

ウ. 一つのルールに対して、2,000 件以上のフィルター条件を登録できること。また、運用への負荷を増やさずにフィルタリングポリシーが妥当性を判別できるようにルール設定後は仮運用(テストモード)によって、実際のルール設定が妥当であるかどうかをメール流通に影響がない状態で確認ができること。

エ. 汎用ミドルウェアの導入・運用コストを軽減するため、メール保存については、SQL サーバー、My SQL 等、外部データベースの利用を必要としないこと。さらに、保存メールはメール件名、本文だけでなく、添付ファイルも保存できること。また、ファイル移動操作ミスなど意図しない形での保存メール削除などを検知するため、保存メールの改竄検知機能を標準で搭載し、改竄検知はヘッダー、本文の編集だけでなく、メール自体の削除についても検知が可能であること。

オ. 保存したメールを検索する場合、保存メールの検索時には複数のメール保存領域を同時に指定でき、検索結果画面(一覧)でプロトコルの種別(SMTP/POP3)が容易に視認でき、クライアントの障害や災害対策等のために簡易的に復旧できるように、保存メールの検索結果を一括で全件出力(csv/eml 形式)が可能であること。

カ. メールの運用状況を簡単に確認できるレポート機能を有しており、レポート機能はグラフ等によって視覚的、直感的に把握が可能であること。

キ. ソフトウェアのバージョンアップはメジャーバージョンアップを除き管理画面上からのマウス操作で可能であること。

(3)Webフィルタリング

ア. データベースは独自検索エンジンを用いた収集を行い、専任部門による目視確認が行われていること。また、データベースはマルウェア(スパイウェア)、フィッシング等へのサイトに対応しており、なおかつ、フィルタリング URL データベースが 92 カテゴリ以上に分類されていること。

イ. さらに、機密情報の取得を目的とした多様な標的型攻撃から効率的に防御するため、出口対策用の情報は、国内 1,000 台以上のファイアウォール、IDS、IPS、UTM 等の監視センサーによる約 3 億件以上/日のエラーログを 24 時間監視し収集されたものが含まれていること。

ウ. Web サイトへのアクセス制御時には警告画面を表示させることができ、ソフトウェアがアクセス制御機能として提供するユーザー定義リスト、規制カテゴリ等の照合順をユーザーが自由に変更できること。また、グループ毎に異なるフィルタリングポリシーを設定でき、さらにグループ階層構造は 8 階層まで作成できること

エ. 通信では同一スペック上の筐体で動作させた場合の Squid(OSS プロキシ)より高い通信処理能力を有すること。さらに、上位のプロキシサーバーを複数台指定でき、各プロキシサーバーのアクティブ/スタンバイ設定、ラウンドロビンを含む任意の転送比

率指定が行えること。また、IPv6 のインターネットサイトに対応していること(LAN 側 IP を除く)。Web サイトへのアクセス時は、任意のヘッダーを特定の文字列に変更できること。

オ. ログを単に取得するだけでなくインフラ環境の効率的な運用に役立てるため、アクセスログについては、「日時」「クライアント」「グループ」「カテゴリ」「URL」等で抽出が可能なログ検索ツールが用意されており、さらに改竄検知機能を有し、ログが人為的に修正されてないことを証明できること。また、「ブロックログ」はリアルタイムで出力され、ブロックログから直接ユーザー定義する URL リストにワンクリックで登録が可能なこと。「POST ログ」では HTTPS サイトを通じて送信されたファイルが規制した、しないに関わらず記録の復元が可能であること。SSL 通信の際、https サイトの任意のヘッダを元に Facebook や twitter 等任意のアカウントの制限が可能なこと。

カ. SSL 通信についてはカテゴリによって SSL 通信の解析結果を記録する/しない が選択できること。管理上は、Web フィルタリングの設定は Web ブラウザ経由でアクセスする管理画面からリモートで管理でき、さらに設定の変更履歴を詳細に記録し、変更前、変更後の内容を管理画面から簡単に確認できること。また、現状の設定内容を的確に把握し、運用管理に役立てるため、フィルタリングポリシーの設定状態を PDF ファイルで出力する機能を有すること。

9. 役務仕様

(1) 基幹系サーバ

ア. 適応範囲

指定するソフトウェア機能を用いて受託業者が最良な提案を行い、広報情報課の承諾を得て導入すること。

以下の機能利用を想定している。

a) 資産管理
b) ソフトウェア資産管理
c) デバイス管理
d) ログ管理
e) セキュリティ管理
f) 各種レポーティング

イ. 役務内容

以下の役務を主に実施するものとする。

a) ＯＳ環境設計、インストール、環境設定
b) 利用を想定する各機能の環境設計、インストール、環境設定
c) 上記機能のテスト
d) 上記 a)～c)に関連するドキュメント作成

・設計書

・設定パラメータシート

・テスト計画書

・テスト仕様書

・運用マニュアル

ウ. 留意事項

以下の事項に留意するものとする。

a）本サーバの環境設計については、受託業者が最良な提案を実施し広報情報課の承諾を得ること。

b）その他条件を満たす為に必要なソフト、機器等は納入業者にて用意することとする。

(2)情報系サーバ

ア. 適応範囲

指定するソフトウェア機能を用いて受託業者が最良な提案を行い、広報情報課の承諾を得て導入すること。

以下の機能利用を想定している。

a）電子メールのアーカイブと検索

b）電子メールの送受信制御

c）Webフィルタリング

d）Webコンテンツフィルタ

e）USBデバイス管理

・基幹系のクライアントＰＣだけでなく、情報系のクライアントＰＣについても、管理されていないＵＳＢデバイスが接続されるのはセキュリティ上好ましくないため、情報系にも専用のＵＳＢデバイス管理システムを導入することで対応する。サーバや管理用端末が必要な場合は調達範囲内とする。ただし、既存の機器（今回導入予定のサーバを含む）を利用できるのであれば納入前に申告すること。

イ．役務内容

以下の役務を主に実施するものとする。

a）ＯＳ環境設計、インストール、環境設定

b）利用を想定する各機能の環境設計、インストール、環境設定

c）メール転送機能の設定

・調達前のメール転送フロー

情報系クライアント　→　ファイアウォール　→　メールサーバ（レンタル）　→　インターネット

・調達後のメール転送フロー

情報系クライアント　→　メールフィルタリング用サーバ　→　ファイアウォール　→　メールサーバ（レンタル）　→　インターネット

・情報系クライアントの設定変更

情報系クライアントのメールソフト設定（SMTP/POP3）を「メールフィルタリング用サーバ」に変更

・通信機器の設定変作業支援

ファイアウォールの LAN 側からのメール関連のアクセスを「メールフィルタリング用サーバ」のみに変更する作業支援

d）Web 閲覧機能の設定

・調達前の Web 閲覧フロー

情報系クライアント　→　ファイアウォール　→　インターネット

・調達後の Web 閲覧フロー

情報系クライアント　→　Web フィルタリング用サーバ　→　ファイアウォール　→　インターネット

・情報系クライアントの設定変更

情報系クライアントのブラウザ設定（プロキシ）を「Web フィルタリング用サーバ」に変更する。

・通信機器の設定変作業支援

ファイアウォールの LAN 側からの Web 閲覧関連のアクセスを「Web フィルタリング用サーバ」のみに変更する作業支援

e）上記機能のテスト

f）上記 a)～e)に関連するドキュメント作成

・設計書

・設定パラメータシート

・テスト計画書

・テスト仕様書

・運用マニュアル

ウ. 留意事項

以下の事項に留意するものとする。

a）本サーバの環境設計については、受託業者が最良な提案を実施し広報情報課の承諾を得ること。

b）その他条件を満たす為に必要なソフト、機器等は納入業者にて用意することとする。

(3)共通

ア. 各サーバのデータバックアップ運用について、受託業者が最良な提案を実施し広報情報課の承諾を得て環境を構築すること。

イ．各サーバの全データのバックアップを実施すること（本バックアップデータはハードウェア障害等の惨事復旧に利用できること）また、システム機能上で重要なデータは日々のデータバックアップ運用に組み込むこと。

ウ．機器の搬入は広報情報課と相談の上、業務等に支障をきたすことがないようにすること。また、作業のなかで生じた問題については、広報情報課の指示に従うこと。

エ．納入時に発生する空き箱等の残材は、納入業者が責任をもって処分すること。

オ．納入機器等には、取扱説明書、保証書等を添付すること。

カ．搬入等に係る費用の一切を含むこと。

キ．納入時には、全体作業の責任者を定めるとともに、各々の作業について責任者（全体責任者が現場にいる場合は、兼任も可）を定め、作業時には名札を付けること。

ク．納入時には、サーバ本体に広報情報課が提供するシールを貼り付けること。

ケ．機器調達については、大和高田市役所内に構築されたＬＡＮで使用できるように、ネットワークの接続及び設定を行うこと。

コ. 別途指示する設定情報を元に、コンピュータ名及び管理者等の設定を行うこと。また、ユーザー情報の作成を行うこと。

サ. 今回導入に伴い発生する端末作業（プロキシ設定、資産管理クライアントの導入等）に係る費用は、全て受託業者が負担すること。

シ. テスト計画書を作成し、テスト実施前に広報情報課にてテスト項目の確認及び承諾を得ること。また、テスト完了時はテスト結果を広報情報課に報告し、承諾を得ること。

(4)移行・切り替え

ア．各サーバ、ネットワーク機器の移行及び切り替えについては安全性を含め、以下を十分に考慮し行うこと。また、移行・切り替えの手法、スケジュール等の内容詳細については事前に計画書を作成し、広報情報課と協議の上、決定とする。

a）稼動業務への影響

b）稼動業務の運用スケジュール

c）進捗遅延や切り替え時のトラブル発生による環境切り戻し

（５）運用

ア．各サーバの運用管理に必要なハードウェア及び、ソフトウェアの簡易操作マニュアル、障害対応マニュアルを作成し提供すること。また、内容の詳細等については広報情報課と協議の上、決定とする。

イ．各サーバについて、バックアップやログ管理等の日常的に管理する必要性のある運用業務について運用マニュアルを作成し提供すること。また、内容の詳細等については広報情報課と協議の上、決定とする。

ウ．各サーバ、ネットワーク機器を運用するにあたり、広報情報課に対し十分な研

修を行うこと。また、内容の詳細等については広報情報課と協議の上、決定とする。

10．保守仕様

ア．ハードウェア保守

a）サーバの保守業者は、本市設置場所へ公共交通機関等を利用して60分以内で移動できる場所に保守拠点を有すること。

b）初期不良等の場合は、迅速な対応を行い、使用可能な状態に復旧すること。

c）広報情報課に対して連絡体制を明確にし、広報情報課から故障等の連絡のあった場合は、出張修理を基本とし、状況を把握し迅速な対応を行うこと。

d）納入機器については、導入後5年間のメーカー保守を行い、機器の故障等が発生した場合は、無償でシステム復元とデータ復旧を行うこと。

e）メーカーとの保守契約に必要な登録作業は、納入業者が行うこと。

f）納入する機器の保守業者は、プライバシーマーク又は ISMS 認証を取得していること。

g）納入機器の保守対応については、土曜日、日曜日及び祝日並びに12月29日から翌年1月3日までの日を除く9時から17時までとし、障害の連絡を行った当日の作業開始を原則とする。なお、復旧作業に時間を要し、17時を超えた場合は、対応時間外においても復旧作業を継続するものとする。また、致命的な障害等で対応が緊急に必要であると保守業者が判断した場合、若しくは、本市からの申出があった場合には、受付対応時間及び作業対応時間を延長できるものとする。

h）本体引上げによる修理が必要な場合は、保守業者持込みの代替機とハードディスク等記憶媒体を入れ替えるなどの処置をとり、ハードディスクを引き上げることの無いようにすること。なお、ハードディスクが故障した場合、故障したハードディスクは、保守業者の責任において記録情報の完全消去・物理的破壊・暗号化等読取りできないように処置し、その事実を確認できる書類を広報情報課に提出すること。

i）受付方法は、専用コールセンターへの電話／FAX／E－MAILによる対応とする。

イ．システムエンジニアサポート

稼動後 5 年間のシステムエンジニアサポート費用を含むこと。

サポート条件は以下の通りとする。

・対応時間は平日9:00～17:00とする。

・本事業導入機器、ソフトウェア(OS含む)及びパッケージシステム全般に関する問題解決支援とする。

（問い合わせ先）

大和高田市広報情報課情報管理係　電話0745－22－1101（内線319）

以上